TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvement

February 7, 2017

Reference Number: 2017-40-017

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
2 = Risk Circumvention of Agency Regulation or Statute

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

EFFORTS CONTINUE TO RESULT IN IMPROVED IDENTIFICATION OF FRAUDULENT TAX RETURNS INVOLVING IDENTITY THEFT; HOWEVER, ACCURACY OF MEASURES NEEDS IMPROVEMENT

Highlights

Final Report issued on February 7, 2017

Highlights of Reference Number: 2017-40-017 to the Internal Revenue Service Commissioner for the Wage and Investment Division.

IMPACT ON TAXPAYERS

Identity theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number to file a fraudulent tax return. Unscrupulous individuals steal identities for use in submitting tax returns with false income and withholding documents for the sole purpose of receiving a fraudulent tax refund.

WHY TIGTA DID THE AUDIT

The IRS's Identity Theft Taxonomy measures its efforts to defend against identity theft and to identify areas requiring additional effort. This audit was initiated to assess the effectiveness of the IRS's continued efforts to detect and prevent identity theft, measure undetected identity theft, and coordinate identity theft information with other Government agencies and tax industry partners.

WHAT TIGTA FOUND

Recognizing the impact that identity theft has on tax administration, the IRS continues to adopt strategies to improve detection and prevention. While these strategies have led to many notable improvements, identity theft continues to evolve and become more sophisticated. As such, the IRS began to explore other initiatives that would assist with its overall detection and prevention efforts such as convening a Security Summit, coding of Forms W-2, *Wage and Tax Statement*, *etc*.

TIGTA identified continued reductions in the volume of undetected potentially fraudulent tax returns. TIGTA identified 568,329 Tax Year 2013 undetected potentially fraudulent tax returns with tax refunds totaling more than $1.6 billion, a reduction of more than $523 million from the prior year. However, the false reporting of wages and withholding continues to account for the largest amount ($1.3 billion) of undetected potentially fraudulent tax return refunds. With the passage of legislation to accelerate the reporting of Forms W-2, the IRS should be able to significantly reduce the number of these undetected tax returns.

TIGTA also identified that using State lead data during tax return processing can improve identity theft detection efforts. Finally, TIGTA found that the accuracy of the Identity Theft Taxonomy quantification for both protected and unprotected revenue could be improved. For example, the IRS's estimate of protected revenue was overstated by almost $2.4 billion resulting from the incorrect calculation of refunds associated with rejected electronically filed tax returns.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS expand the use of its identity theft models to include all accelerated Forms W-2, develop a process to use State lead data, and update the Identity Theft Taxonomy methodology used to quantify unprotected and protected revenue.

IRS management agreed with all of TIGTA's recommendations. The IRS indicated that it programmed the Return Review Program to include all accelerated Forms W-2 received from the Social Security Administration for Tax Year 2016, implemented a process to use State lead data, modified the methodology for rejected tax returns, updated the Identity Theft Taxonomy methodology to remove duplications of tax returns, and has plans to further revise the methodology to improve the accuracy of the unprotected identity theft estimates.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

February 7, 2017

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvement
(Audit # 201540001)

This report presents the results of our review to assess the effectiveness of the Internal Revenue Service's continued efforts to detect and prevent identity theft, measure undetected identity theft, and coordinate identity theft information with other Government agencies and tax industry partners. This audit was included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Fraudulent Claims and Improper Payments.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services).

Table of Contents

Appendices

Abbreviations

e-file(d)	Electronically file(d)
IRS	Internal Revenue Service
PY	Processing Year
RRP	Return Review Program
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TY	Tax Year

Background

Identity theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number[1] to file a fraudulent tax return. Unscrupulous individuals steal identities for use in submitting tax returns with false income and withholding documents to the Internal Revenue Service (IRS) for the sole purpose of receiving a fraudulent tax refund.

To identify fraudulent tax returns involving identity theft and prevent refunds from being issued, the IRS uses various detection systems such as the Dependent Database[2] and the Return Review Program (RRP).[3] Once identified by these detection systems, tax returns are held from processing and the IRS sends a notice to the taxpayer at the address on the identified tax return. The notice requests that the taxpayer confirm his or her identity with the IRS. If the taxpayer's identity is confirmed, the IRS removes the hold on the tax account which allows the tax return to continue processing and the issuance of any refund due. If the taxpayer's identity is not confirmed, the IRS removes the tax return from further processing and places an identity theft indicator on the taxpayer's account for future reference.

The IRS's efforts to quantify identity theft

The Treasury Inspector General for Tax Administration (TIGTA) first reported in July 2012[4] that the impact of identity theft on tax administration is significantly greater than the amount the IRS detected and prevented. While the amount of fraudulent tax refunds that the IRS detected and prevented was substantial, it did not have a process to measure how many identity thieves were filing fictitious tax returns and how much revenue was being lost due to the issuance of fraudulent tax refunds. The IRS initiated the Identity Theft Taxonomy research project to measure the IRS's efforts to defend against identity theft as well as to identify areas requiring additional effort. The IRS published the first Identity Theft Taxonomy report on September 15, 2014, and continues to annually update the Identity Theft Taxonomy analysis to:

[1] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, it can be an Employer Identification Number, a Social Security Number (SSN), or an Individual Taxpayer Identification Number.
[2] The Dependent Database is a rules-based system that incorporates information from many sources that include the Department of Health and Human Services, Social Security Administration, and the IRS.
[3] The RRP uses predictive analytics, models (*i.e.*, filters), clustering, a scoring system, business rules, and selection groups to identify suspected identity theft and fraudulent tax returns.
[4] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

- Provide the IRS with a quantifiable measure of overall identity theft detection and prevention efforts.
- Identify and quantify identity theft not detected by its filters. These tax returns are then analyzed to refine existing or build new identity theft detection filters.

The September 15, 2014, Identity Theft Taxonomy reported that the IRS's efforts protected between $22 billion and $24 billion in fraudulent tax refunds from being issued in Processing Year (PY)[5] 2013. The IRS refers to this in its Identity Theft Taxonomy report as "protected revenue." However, the IRS also reported that identity thieves were successful in receiving approximately $5.75 billion in fraudulent tax refunds. The IRS refers to this in its Identity Theft Taxonomy report as "unprotected revenue."

The IRS improved its Identity Theft Taxonomy analysis for identifying and quantifying unprotected revenue in PY 2014

The IRS recognizes that new identity theft patterns are constantly evolving. As such, it has continued to adapt its detection and prevention processes as well as revised its methodology for identifying and quantifying unprotected revenue for the PY 2014 analysis as follows:

- Revised its analysis based upon tax returns that were identified as confirmed identity theft, but the tax refunds were issued prior to the tax return being identified as confirmed identity theft and were not recovered.
- Developed a methodology to better identity and quantify tax returns with characteristics of identity theft that its filters missed.
- Captured specific tax return information from analysis of potential identity theft tax returns to build, modify, and test identity theft filters.

On September 25, 2015, the IRS published the Identity Theft Taxonomy report of its analysis of tax returns processed in PY 2014. Figure 1 show results the IRS reported to quantify protected and unprotected tax revenue for PY 2014 tax returns involving identity theft. Due to the differences in the calculation of unprotected tax revenue, the IRS's analysis for PY 2014 cannot be compared to the results for PY 2013.

[5] The processing year is the calendar year in which the tax return or document is processed by the IRS.

Figure 1: IRS Analysis of Revenue Protected and Unprotected by the IRS's Identity Theft Detection Processes During PY 2014

	Protected Tax Revenue		Unprotected Tax Revenue	
PY	Tax Returns (Millions)	Tax Refunds (Billions)	Tax Returns (Millions)	Tax Refunds (Billions)
2014	3.5	$21.5	1.2	$3.1

Source: The IRS Return Integrity and Compliance Services Division analysis of identity theft, dated September 25, 2015.

Legislation was passed to accelerate income and withholding information

In our July 2012 audit, we reported that access to third-party income and withholding information at the time tax returns are processed is the single most important tool that the IRS needed to further its efforts to identify and prevent tax refund fraud. In April 2015,[6] we again expressed our concerns over timely access to third-party income and withholding information. We found that while the IRS had made improvements in its detection efforts, the IRS did not have timely access to third-party income and withholding information because most of the third-party income and withholding information is not received by the IRS until well after tax return filing begins. For example, the deadline for filing most information returns with the Social Security Administration is March 31, yet taxpayers can begin filing their tax returns as early as mid-January each year. For the 2014 Filing Season, the IRS received approximately 90.8 million tax returns as of March 28, 2014.

On December 18, 2015, the President signed the Consolidated Appropriations Act of 2016[7] which contained provisions to help combat identity theft. The Act requires employers to submit third-party income and withholding information, *i.e.*, Forms W-2, *Wage and Tax Statement*, and any returns or statements required to report nonemployee compensation, on or before January 31 of the following tax year. This will be effective for Tax Year (TY) 2016, and third-party income and withholding documents are required to be submitted to the Social Security Administration on or before January 31, 2017.

This review was performed as a follow-up review to the April 2015 TIGTA audit on identity theft and was performed with information obtained from the IRS Wage and Investment Division Accounts Management, Return Integrity and Compliance Services function in Atlanta, Georgia, during the period January through October 2016. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable

---

[6] TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).
[7] Pub. L. No. 114-113.

basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Recognizing the impact that identity theft has on tax administration, the IRS continues to adopt strategies focused on improving its detection and prevention of identity theft. While these strategies have led to many notable improvements, it became clear to the IRS that identity theft continues to evolve and become more sophisticated. As such, the IRS began to explore other initiatives that would assist with its overall detection and prevention efforts. These initiatives include:

- ***Convening a Security Summit to discuss common challenges and ways to leverage collective resources and efforts for identity theft detection and prevention.*** The Security Summit is a collaborative effort of IRS officials, the Chief Executive Officers of leading tax preparation firms, software developers, payroll and tax financial product processors, and representatives from State Departments of Revenue.

  As a result of the Security Summit, the IRS began receiving 23 new data elements with electronically filed (e-filed) tax returns during PY 2016 to further its efforts to detect and prevent identity theft. The IRS tested and used three of the new data elements during PY 2016 in the RRP to systemically identify potential identity theft tax returns. In September 2016,[8] TIGTA reported that as of March 25, 2016, the IRS identified potential identity theft on approximately 21,000 tax returns claiming $72 million in tax refunds using these three new data elements. The IRS is evaluating the remaining 20 data elements for future filter development.

- ***Obtaining early submission of Forms W-2.*** In PY 2016, the IRS initiated a voluntary program in which 18 payroll providers were requested to submit Forms W-2 directly to the IRS by January 31, 2016. The IRS used the RRP identity theft models to compare the Form W-2 information to the tax return at the time the tax return was processed for identity theft detection. The IRS stated that as of April 25, 2016, it selected 15,624 tax returns for identity theft treatment based upon the early submission of Forms W-2, and equally as important, it excluded 33,628 tax returns from identity theft treatment because the income information matched.

- ***Using verification codes on Form W-2 to improve efforts to validate income and withholding information.*** The IRS initiated a pilot during PY 2016 to test the feasibility of using a verification code to authenticate Form W-2 data. The IRS identified four large payroll providers to participate in its Form W-2 verification test. The payroll providers were responsible for placing a verification code on the Form W-2. The IRS provided the payroll

[8] TIGTA, Ref. No. 2016-20-062, *Filing Season 2016: Implementation of New Data Elements* (Sept. 2016).

providers with the specifications required to generate a 16-digit verification code that is placed on all employees' Forms W-2 of selected employers. The employee (or employee's tax preparer) is then asked to provide the verification code when preparing the tax return using tax preparation software. The IRS is conducting a post-filing season review to evaluate the use of a Form W-2 verification code.

- ***Obtaining leads of potential identity theft tax returns from State tax agencies and tax industry partners.*** The IRS piloted the State Suspicious Filer Exchange in PY 2013. Through this program, the States provide the IRS referrals of potential and confirmed identity theft, tax return preparers connected to the filing of potential identity theft tax returns, and other fraudulent activities that the States identified during the processing of the State tax returns. During PY 2015, the IRS received 105,684 unique taxpayer Social Security Numbers (SSN) through the State Suspicious Filer Exchange.

  The IRS also expanded its industry lead program to require industry partners to perform regular reviews to identify possible identity theft schemes and report them to the IRS to help stay on top of emerging schemes. In August 2015, the IRS updated requirements for authorized e-file providers requiring transmitters who collectively transmit more than 2,000 individual income tax returns per year to perform post-filing analytics and provide data to the IRS on identity theft refund fraud patterns. According to the IRS, during PY 2016, identity theft filters selected 203,000 tax returns with more than $1 billion in refunds claimed that were also submitted as potential identity theft by industry partners.

As part of our ongoing identity theft audit coverage, we plan to assess the IRS's continued implementation of these various initiatives. In addition to implementing its own initiatives, the IRS continues to take action in response to prior TIGTA recommendations. These actions include:

- Implemented new and refined clustering filters that use address and bank account numbers.
- Expanded identity theft filters to increase its identification of identity theft involving ***************************2*****************************.

Analysis Identified Continued Reduction in Undetected Potentially Fraudulent Tax Returns

Our review of TY 2013 tax returns identified continued reductions in the volume of undetected tax returns with characteristics of IRS-confirmed identity theft cases. We identified 568,329 TY 2013 undetected potentially fraudulent tax returns with tax refunds totaling more than $1.6 billion.[9] Our analysis showed that potential undetected identity theft has decreased by 219,014 tax returns totaling more than $523 million from TY 2012 to TY 2013. However, the false reporting of wages and withholding continues to account for the largest amount of undetected potentially fraudulent tax returns with refunds totaling more than $1.3 billion. With the passage of legislation to accelerate the reporting of Forms W-2 and IRS use, the IRS should be able to significantly reduce the number of undetected tax returns reporting false wages and withholding if it compares the accelerated Form W-2 information to the tax return at the time the tax return is processed. Figure 2 summarizes our four-year analysis, including the types of ***2******* reported.

Figure 2: Comparisons by Tax Year of Type of ******2*** Claimed on the Undetected Potentially Fraudulent Tax Returns**

Type of ***2*** ***2*** Reported		TY 2010	TY 2011	TY 2012	TY 2013
2	Tax Returns	1,128,531	802,672	607,481	483,323
	Tax Refunds	$3,495,621,793	$2,354,349,943	$1,511,910,501	$1,324,664,815
*********2******** ********2*******	Tax Returns	93,142	12,993	3,064	1,814
	Tax Refunds	$231,692,282	$62,856,556	$8,151,222	$777,150
*****2**** *****2*****	Tax Returns	154,729	204,522	175,191	83,133
	Tax Refunds	$531,293,018	$698,118,714	$611,279,472	$288,142,460
********2********	Tax Returns	115,813	66,811	1,607	59
	Tax Refunds	$962,411,091	$497,081,019	$6,056,787	$316,414
Total	**Tax Returns**	**1,492,215**	**1,086,998**	**787,343**	**568,329**
	Tax Refunds	**$5,221,018,184**	**$3,612,406,232**	**$2,137,397,982**	**$1,613,900,839**

Source: TIGTA's analysis of TYs 2010, 2011, 2012, and 2013 tax returns.

The characteristics we used to identify potentially undetected fraudulent tax returns are based on IRS-confirmed identity theft tax returns and are the same characteristics we have used for the four years we have conducted this assessment. Identity thieves and the characteristics they use to submit fraudulent tax returns continue to evolve. As such, the characteristics we use for our analysis are not all inclusive. We have used our analyses for comparison purposes to assess the IRS's efforts to improve its detection of identity theft tax returns. Figure 3 provides a summary of the characteristics of the SSNs used on the undetected tax returns we identified.

[9] Although these tax returns met the characteristics of IRS-confirmed identity theft cases involving the use of an SSN, some potentially fraudulent tax returns we identified could also be the result of nonreporting of income and withholding by the employer or an individual using his or her own SSN to file a fraudulent tax return.

Figure 3: Characteristics of the Individuals Whose SSNs Were Used on Undetected Potentially Fraudulent Tax Returns

Characteristic	Tax Returns	Tax Refunds Issued
Children (under age 14)	908	$582,925
Citizens of U.S. Possessions	7,756	$32,288,806
Deceased Individuals	5,192	$6,686,984
Elderly Individuals (age 70 and older)	4,242	$5,724,296
********************2**************************[10]	422,514	$1,345,673,963
Prisoners	7,354	$18,053,640
Students (ages 16 to 22)	120,363	$204,890,225
Total	**568,329**	**$1,613,900,839**

Source: TIGTA's analysis of TY 2013 tax returns.

The IRS should **********2****************in its identity theft detection efforts

Notwithstanding the improvements previously cited, our analysis of the 568,329 undetected potentially fraudulent TY 2013 tax returns identified 70,065 tax returns (12 percent) that ***2** *************2************* the IRS established to select a potentially fraudulent tax return for review. Refunds associated with these tax returns totaled almost $13.1 million. Expanding our analysis to all TY 2014 tax returns, we identified that 15.7 million taxpayers had ***2*** ******************2********************and claimed more than $3 billion. Of these, 121,375 tax returns with refunds issued totaling $24.3 million had addresses that matched the address of other tax returns identified as confirmed identity theft.

On January 7, 2016, prior to the start of PY 2016, we brought to IRS management's attention our concern about excluding tax returns with ********************2******************** **********************************2*** ***********2*********. IRS management stated that they did not want to change the model for PY 2016 because they did not have enough data to fully understand the impact on false positives.[11] IRS management also stated that when the ***********2************* *********,[12]****************************2************************************** ***************************2*************************. However, the IRS noted that its Integrity and Verification Operations Fraud and Referral Evaluation group does select tax returns with *****************2**************************. Further, the IRS indicated

[10] This category contains tax returns filed with income claimed for *****************2****************** that would indicate the legitimate taxpayers did not have************2*************.

[11] A false positive identity theft case refers to a case identified as potential identity theft, but the verification confirms the identity of the taxpayer.

[12] The 12-consecutive-month period ending on December 31.

that they have analyzed tax return information and are considering the creation of a model specifically geared toward ********************2************************* *******2*******. In addition, the IRS stated that it implemented a filter for tax returns filed after April 21, 2016, that selected tax returns ************2******************** ********************2***************************.

Using State lead data during tax return processing can improve identity theft detection efforts

As previously discussed, the IRS analyzes State lead data looking for questionable filing patterns for identity theft filter development. However, it does not have a process to expedite the use of this data as it is received during the filing season. For example, our analysis identified 90,341 SSNs received from State leads during the 2015 Filing Season that filed a TY 2014 tax return. For 83,717 (93 percent) of the SSNs, the lead was not in time for the IRS to take action, *i.e.*, a tax return was already processed for the individuals. However, for 6,624 (7 percent) of the 90,341 SSN referrals, the information was received within a time frame that would have allowed the IRS to identify and review the individual's tax return during processing, *i.e.*, the tax returns had not already been processed. The IRS issued refunds for 4,418 of the 6,624 tax accounts totaling more than $20 million. The IRS is missing an opportunity to identify and prevent potential identity theft on current tax year tax returns.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Expand the use of the RRP identity theft models to include all accelerated Forms W-2 information for comparison to tax returns at the time they are processed for identity theft detection and to exclude, from identity theft treatment, tax returns where the income information matched.

> ***Management's Response:*** The IRS agreed with this recommendation and began using accelerated wage and withholding information during the 2016 Filing Season. In addition to the data received from payroll providers, the RRP also had access to wage and withholding information from Forms W-2 transmitted by the Social Security Administration. Upon the IRS's receipt and posting to the Information Returns Master File,[13] the RRP used the data to identify questionable returns that may have been potentially fraudulent. The RRP programming became active on January 19, 2016, and no new programming is required to take advantage of the wage and withholding information that will be due by January 31, 2017, for TY 2016.

[13] An IRS database that contains third-party information documents for taxpayers such as Form W-2.

Recommendation 2: Develop criteria to identify and evaluate for fraud potential tax returns ****************2*************************************

> **Management's Response:** The IRS agreed with this recommendation. On June 13, 2016, the IRS implemented a new business rule within the Dependent Database ****************************2**************************************
> *****2***.

Recommendation 3: Develop a process to timely use State lead data as another characteristic in evaluating tax returns during processing to identify potential identity theft tax returns.

> **Management's Response:** The IRS agreed with this recommendation. On January 8, 2017, the IRS implemented programming within the RRP that permits it to consider previous State lead data in informing the teams responsible for evaluating filter and model effectiveness.

Improvements Are Needed to Increase the Accuracy of Some Identity Theft Estimates Reported in the Identity Theft Taxonomy

Our review of the IRS's Identity Theft Taxonomy analysis of TY 2013 tax returns found that the IRS's methodology provides a reasonable basis for identifying and quantifying potential undetected identity theft tax returns. However, the accuracy of the quantification for both protected and unprotected revenue could be improved. Specifically, we identified that the IRS's estimate of total revenue protected of $21.5 billion was overstated by almost $2.4 billion (11.3 percent). The overstatement was the result of the IRS using an estimate of the amount associated with refunds protected from the rejection of e-filed tax returns. The IRS's Identity Theft Taxonomy measure of revenue protected includes rejected e-filed tax returns in which the rejection of the tax return relates to identity theft. For example, tax returns filed using a deceased individual's SSN are rejected from IRS processing. The IRS identified more than 1.2 million rejected tax return submissions from internal reports and applied an average refund amount of $5,959[14] to arrive at its estimate for revenue protected from the rejection of e-filed tax returns. However, the IRS has data available which provide the actual refund amount for rejected tax return submissions. Using these data, our review of more than 1.2 million rejected tax return submissions identified the following overstated amounts:

- $1.8 billion – we identified 891,645 unique rejected tax return submissions claiming actual refunds totaling almost $3.5 billion. The IRS used its average refund amount ($5,959) to calculate the total revenue protected as $5.3 billion for these 891,645 tax returns.

[14] This is the average refund amount for all confirmed identity theft cases.

- $479 million – we identified 80,496 tax returns with a balance due or zero balance due that should have been excluded from the IRS's estimate of revenue protected.
- $91 million – we identified 15,290 rejected tax returns that should have been excluded from the IRS's estimate of revenue protected because they had already been included in the IRS's calculation. These involved tax returns that were rejected for more than one reason and the IRS's estimate included the same tax return for each identity theft-related reject reason.

When we brought these concerns to the IRS's attention, IRS management advised that they are revising the methodology used to estimate revenue protected by the IRS's e-file rejects to address the concerns we reported. The IRS did explain that the data file used by TIGTA was not used by the IRS because some of the data file was corrupted. It should be noted that the corrupted files account for 231,853 of the rejected tax return submissions. However, the IRS would have been able to accurately identify the refund amounts associated with the remaining 987,431 tax return submissions if they had used this file.[15] The IRS agreed that the reject conditions for tax returns that do not claim a refund should not be included in revenue protected and tax return submissions with multiple reject conditions should be included only once. Additionally, the IRS acknowledged the average refund amount may not be representative of the population of e-file rejects.

The IRS erroneously included refunds for the exact same tax returns in both protected and unprotected revenue

Our analysis also identified 16,292 tax returns that were included in both the protected and unprotected revenue categories. This resulted in an overstatement of protected revenue of more than $55.4 million. These tax returns involved ones where the IRS identified the tax return as potentially fraudulent, but the refund had already been issued. The IRS's Identity Theft Taxonomy measures of revenue protected and unprotected should include a tax return in only one category to avoid double counting. When we brought this to the IRS's attention, the IRS agreed it double-counted these tax returns and indicated it will exclude tax returns from the confirmed identity theft estimate that are also identified in the unprotected revenue estimate.

---

[15] Our analysis identified a total of 1,219,284 rejected tax return submissions. However, 231,853 rejected tax return submissions had missing details of tax return data due to corrupted data files that the IRS could not recover. This could represent an additional overstatement of revenue totaling almost $477 million assuming the same average refund of $3,903 determined by our review of 891,645 with data available are applied. This average excludes 80,496 tax returns with a balance due or zero balance due and 15,290 rejected tax returns rejected for more than one reason. This additional overstatement is not included in our total overstatement of $2.4 billion.

Errors in the methodology for identifying income discrepancies resulted in the incorrect identification of potential tax returns involving identity theft

Our analysis also identified 40,947 tax returns that were erroneously included in the IRS's Identity Theft Taxonomy analysis as potential identity theft tax returns not detected by the IRS's identity theft filters. Inclusion of these tax returns resulted in an overstatement of unprotected revenue of more than $82.7 million. This resulted from errors in the IRS's calculation and comparison of income and withholding reported on Forms W-2 to income and withholding reported on the associated tax return. The IRS's Identity Theft Taxonomy methodology to identify revenue unprotected did not account for amended or duplicated Forms W-2 in its calculation and comparison of income and withholding.

The IRS receives and maintains both original and amended Forms W-2. In the IRS's income summing process, total wages and Federal tax withholding from the original and amended Forms W-2 are added together for matching to the income reported on the associated tax return. As a hypothetical example,[16]

> *Employer A issues Employee B a Form W-2 reporting wages of $40,000 and Federal tax withholding of $3,991. Employer A later finds out that it did not include State tax withholding on Employee B's Form W-2. As such, Employer A files an amended Form W-2 with both Employee B and the Social Security Administration reporting wages of $40,000, Federal tax withholding of $3,991 and State tax withholding of $1,056. In the IRS's income summing process, the IRS erroneously includes both the original and amended Forms W-2 and shows wages of $80,000, Federal tax withholding of $7,982, and State tax withholding of $1,056 which is then used to compare to tax return data reporting only $40,000 of wage income and Federal tax withholding of $3,991.*

When we brought this concern to IRS management's attention, the IRS agreed that the Identity Theft Taxonomy analysis erroneously included all Forms W-2, including duplicates, in its summing process. This results in the IRS incorrectly identifying the tax return as potential identity theft because of overstated wage and withholding amounts.

[16] This hypothetical example was not drawn from any actual taxpayer's information.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 4: Use actual tax return data to identify the refund amount associated with e-filed rejected tax returns when computing revenue protected, exclude rejected e-filed tax returns that do not claim a refund, and accurately account for tax returns with multiple reject reasons.

> ***Management's Response:*** The IRS agreed with this recommendation. For the 2015 Identity Theft Taxonomy report, issued on November 29, 2016, the IRS modified the methodology to count only one rejected tax return when multiple rejections are logged, and to exclude rejected returns that do not claim refunds.

Recommendation 5: Review both the protected and unprotected revenue to ensure that duplicated tax returns are removed.

> ***Management's Response:*** The IRS agreed with this recommendation. For the 2015 Identity Theft Taxonomy report, issued on November 29, 2016, the IRS modified the methodology to remove the duplications that occurred when potentially fraudulent returns were selected by more than one fraud detection system.

Recommendation 6: Exclude tax returns from potential undetected identity theft when mismatches of tax return income are due to amended or duplicate income documents.

> ***Management's Response:*** The IRS agreed with this recommendation and has made improvements in the recently issued 2015 Identity Theft Taxonomy report of protected and unprotected identity theft refund fraud. The methodology changes partially address the estimation errors associated with amended tax returns or duplicate income documents. The IRS will further revise the methodology to improve the accuracy of the unprotected identity theft range estimate.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS's continued efforts to detect and prevent identity theft, measure undetected identity theft, and coordinate identity theft information with other Government agencies and tax industry partners. To accomplish our objective, we:

I. Assessed the methodology to ensure that the Identity Theft Taxonomy report provides accurate and reliable information.

   A. Reviewed the procedures to identify the process and criteria used to create the Identity Theft Taxonomy report.

   B. Interviewed IRS management to identify the purpose and goal for measuring how much tax refunds are protected and unprotected through the filing of identity theft tax returns.

   C. Compared the PY[1] 2013 and PY 2014 Identity Theft Taxonomy report methodologies to identify areas of change that will affect the analysis of protected and unprotected revenue associated with identity theft tax returns.

   D. Determined if the PY 2014 Identity Theft Taxonomy report accurately identified potential identity theft tax returns.

      1. Compared the PY 2014 Identity Theft Taxonomy report methodology for identifying potential undetected tax returns to the TIGTA methodology used in our April 2015 audit report[2] for identifying potential undetected tax returns, and evaluated the differences in the methodologies.

      2. Obtained an extract from the IRS of the tax returns identified as unprotected potential identity theft tax identified in the PY 2014 Identity Theft Taxonomy report.

      3. Identified undetected potentially fraudulent tax returns filed by identity thieves for TY 2013 using an SSN and criteria used in the prior TIGTA audit report based on types of income claimed on the tax return, such as ***********2*********** ****************************2*********************.

[1] The processing year is the calendar year in which the tax return or document is processed by the IRS.
[2] TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).

4. Compared the undetected potentially fraudulent tax returns identified by TIGTA in Step I.D.3. to the extract of unprotected tax returns identified in the Identity Theft Taxonomy report. We evaluated the differences between the two populations of potential identity theft tax returns involving amended or duplicated Forms W-2, *Wage and Tax Statement*, and IRS exclusions.

E. Evaluated the undetected potentially fraudulent identity theft tax returns to identify the types of taxpayers identified as potential identity theft victims *e.g.*, elderly, children, deceased.

F. Assessed other tax return information to determine whether additional tax return characteristics, *e.g.*, ********2******, should be considered by the IRS for identity theft detection.

II. Assessed additional tools the IRS has to help improve identity theft detection and prevention.

A. Determined if the IRS implemented corrective actions in response to our April 2015 audit report.

B. Identified and evaluated results of the 2015 Security Summit.

1. Identified recommendations implemented during PY 2016.
2. Identified the results of implementing new data elements developed in the Security Summit during PY 2016.

C. Assessed the State Suspicious Filer Exchange.

1. Reviewed desk procedures and other internal IRS resources to identify guidance provided to States for providing information to the IRS and IRS guidance for processing information received from State referrals.
2. Determined whether referral information the IRS receives from the State referrals is relevant and useful for the IRS to identify and stop potential identity theft and/or build additional identity theft detection filters.
3. Determined how the IRS identifies and works taxpayer accounts from these referrals.
4. Evaluated the IRS process for using the referral information in its analysis for further development of identity theft fraud filters.

D. Assessed the IRS's plans for obtaining and using tax industry identity theft refund fraud pattern analysis.

E. Discussed with the IRS the progress of the Form W-2 verification pilot program and obtained statistics on the Forms W-2 containing the verification code.

F. Researched the IRS's use of early third-party income documents and determined whether the documents are being used in the RRP for systemic identity theft detection.

G. Discussed the impact of implementing the early third-party income and withholding information for PY 2017 including the IRS's plans for using this information in its identity theft detection efforts. We identified legislation that has passed to accelerate income and withholding information.

Data validation methodology

During this review, we relied on data extracted from the IRS's Individual Return Transaction File[3] for PY 2014 and PY 2015, the Individual Master File[4] for TY 2013 and TY 2014, the National Account Profile database,[5] the Form W-2 File[6] for TY 2013 and TY 2014, and the Refund File[7] for TY 2014 located on the TIGTA Data Center Warehouse.[8] We also relied on a data extract of the IRS's Information Returns Master File[9] database for TY 2013 and the Electronic Tax Administration Research and Analysis System[10] for PY 2014 that was provided by the TIGTA Office of Investigations' Strategic Data Services. We relied on data extracts of TY 2013 tax returns identified by the IRS through the Identity Theft Taxonomy process as potential identity theft, an extract of State leads data from the IRS for PY 2015, and an extract of TY 2014 confirmed identity theft tax returns. Before relying on our data, we ensured that each file contained the specific data elements we requested. In addition, we selected random samples of each extract and verified that the data in the extracts were the same as the data captured in the IRS's Integrated Data Retrieval System.[11] Based on the results of our testing, we believe that the data used in our review were reliable.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the

[3] Contains data transcribed from initial input of the original individual tax returns during tax return processing.
[4] The IRS database that maintains transactions or records of individual tax accounts.
[5] A compilation of selected entity data from various Master Files that also includes data from the Social Security Administration.
[6] The Form W-2 database is created by TIGTA using IRS information reported on Forms W-2 for each tax year.
[7] A database that contains information on tax refunds sent for processing.
[8] A collection of IRS databases containing various types of taxpayer account information that is maintained by TIGTA for the purpose of analyzing data for ongoing audits.
[9] An IRS database that contains third-party information documents for taxpayers such as Form W-2.
[10] A database that contains data from electronic tax returns which includes rejected tax return data.
[11] IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.

following internal controls were relevant to our audit objective: the Identity Theft Taxonomy report which identified the criteria used in identifying protected and unprotected identity theft tax returns and the State leads procedure guide. We evaluated those internal controls by interviewing management, reviewing policies and procedures, and reviewing tax returns identified by the systems.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Diana M. Tengesdal, Director
Darryl J. Roth, Audit Manager
Tom Polsfoot, Supervisory Management and Program Analyst
Jonathan W. Lloyd, Senior Auditor
Quinn A. Major, Auditor
Benjamin D. Meeks, Auditor

Appendix III

Report Distribution List

Commissioner
Office of Commissioner – Attn: Chief of Staff
Deputy Commissioner for Services and Enforcement
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Applications Development
Director, Customer Account Services, Wage and Investment Division
Director, Operations Support
Director, Research, Applied Analytics, and Statistics Business Division
Director, Return Integrity and Compliance Services, Wage and Investment Division
Director, Submission Processing, Wage and Investment Division
Director, Office of Audit Coordination

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; almost $2.4 billion overstatement in the Identity Theft Taxonomy report of protected revenue due to estimating refunds protected from the rejection of e-filed tax returns (see page 10).

Methodology Used to Measure the Reported Benefit:

We obtained a data extract of more than 1.2 million[1] e-filed rejected tax return submissions. We analyzed the tax return information to identify the following overstatements of the revenue protected reported in the Identity Theft Taxonomy report:

- 891,645 unique rejected tax return submissions claiming actual refunds totaling almost $3.5 billion. The IRS used its average refund amount ($5,959) to calculate the total revenue protected as $5.3 billion for these 891,645 tax returns. The IRS estimate of $5.3 billion less the actual refunds of almost $3.5 billion results in an overstatement of $1.8 billion.
- 80,496 tax returns had a balance due or zero balance due and should have been excluded from the estimate. Multiplying the 80,496 tax returns by the IRS's average refund amount ($5,959) results in an overstatement of more than $479 million.
- 15,290 rejected tax returns that should have been excluded from the IRS's estimate of revenue protected because they had already been included in the IRS's calculation. These involved tax returns that were rejected for more than one reason and the IRS's estimate included the same tax return for each identity theft-related reject reason.

[1] Our analysis identified a total of 1,219,284 rejected tax return submissions. However, 231,853 rejected tax return submissions had missing details of tax return data due to corrupted data files that the IRS could not recover. This could represent an additional overstatement of revenue totaling almost $477 million assuming the same average refund of $3,903 determined by 891,645 with data available are applied. This average excludes 80,496 tax returns with a balance due or zero balance due and 15,290 rejected tax returns rejected for more than one reason. This additional overstatement is not included in our total overstatement of $2.4 billion.

Multiplying the 15,290 tax returns by the IRS's average refund amount ($5,959) results in an overstatement of more than $91 million.

We summed the overstatements ($1.8 billion, plus $479 million, plus $91 million) to arrive at a total overstatement of almost $2.4 billion of protected refunds.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; more than $55.4 million overstatement in the Identity Theft Taxonomy report of protected revenue due to tax returns being identified as both protected and unprotected revenue (see page 10).

Methodology Used to Measure the Reported Benefit:

We compared the 1.2 million tax returns identified as unprotected revenue through the Identity Theft Taxonomy analysis with the tax returns identified as confirmed identity theft through the RRP and Dependent Database filters (protected revenue). Our analysis identified 16,292 tax returns that were included in both the protected and unprotected revenue categories. Based on the actual refunds claimed on these tax returns, this resulted in an overstatement of protected revenue of more than $55.4 million.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; more than $82.7 million overstatement in the Identity Theft Taxonomy report of unprotected revenue (see page 10).

Methodology Used to Measure the Reported Benefit:

We conducted an analysis on the 1.2 million tax returns identified as unprotected revenue through the Identity Theft Taxonomy analysis. We identified the Forms W-2, *Wage and Tax Statement*, from the Information Returns Master File for the unprotected tax returns and compared the Forms W-2 and tax return amounts of income and withholding reported. We then identified amended and duplicated Forms W-2 that matched to the tax return for income and/or withholding. Our analysis identified 40,947 tax returns that were erroneously included in the IRS's Identity Theft Taxonomy analysis as undetected identity theft tax returns, and based on the actual refunds claimed on these tax returns, resulted in an overstatement of unprotected revenue of more than $82.7 million.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

JAN 19 2017

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvement (Audit # 201540001)

Thank you for the opportunity to review and provide comments on the subject draft report. We appreciate your acknowledgement of the challenges presented by the constantly evolving threat of identity theft-related tax refund fraud (IDT), and the significant strides we have made in improving our ability to detect potential IDT and commensurately preventing the victimization of taxpayers by IDT, as well as protecting against the revenue loss from IDT.

As part of our strategy for improving IDT detection, the IRS has partnered with industry, tax practitioners, and State governments in sharing information, improving communication, and jointly developing effective countermeasures to constantly changing threats. The Security Summit, a ground-breaking partnership, made great progress in 2016. As a result, we have implemented new safeguards leveraging cooperation with Summit partners, begun working with Summit partners to develop a framework for enhancing cybersecurity protections, and developed an "early warning" system that will help industry, tax practitioner, and State partners quickly identify and share identity theft schemes. Also, the Security Summit partnership has worked to establish an Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) that will be effective for the 2017 filing season and that will assist the members of the Security Summit in detecting and stop IDT fraud.

Because of the Security Summit initiative and our cooperative efforts, we protected more taxpayers from tax-related identity theft, we stopped more suspicious tax returns, and we prevented more fraudulent refunds from getting into criminals' hands. Because of the safeguards enacted by this partnership, fewer people became victims of tax-related identity theft in 2016. Indeed, the Security Summit, along with our continually improved filters, has contributed to our nearly 50 percent decline in identity theft victim receipts this past filing season. For 2017, the emphasis remains on authentication of legitimate tax filers, increased information sharing by partners, and cybersecurity. Most of these activities will be invisible to taxpayers, but will be extremely helpful to Summit partners in detecting and preventing identity theft returns and fraudulent refunds.

In tandem with actions taken to improve IDT detection and stop its occurrence, we have also taken steps to improve our ability to measure the scope of IDT and the amount we are able to stop, as well as improving the accuracy of our estimates of IDT that goes undetected. For improving the accuracy of IDT Protected estimates, we implemented improved methodology that eliminates double-counting when multiple fraud indicators are set by the same return, and more accurately categorizes IDT returns that are not stopped before payment of the fraudulent refund. Our review of returns processed during the 2015 filing season indicated that of total IDT estimated at up to $16.22 billion, we prevented up to $12.88 billion from being paid to IDT criminals. The significant reduction in total IDT from our 2013 and 2014 estimates is attributable to improved detection and estimation methodology.

We agree with the recommendations in the report. Attached are our comments and proposed actions to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Michael Beebe, Director, Return Integrity and Compliance Services, Wage and Investment Division, at (470) 639-3250.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Expand the use of the RRP identity theft models to include all accelerated Forms W-2 information for comparison to tax returns at the time they are processed for identity theft detection and to exclude, from identity theft treatment, tax returns where the income information matched.

CORRECTIVE ACTION
We agree with this recommendation and, as noted in the report, began using accelerated wage and withholding information during the 2016 Filing Season. In 2016, 18 payroll providers voluntarily submitted Forms W-2, Wage and Tax Statement, to the IRS by January 31, 2016. In addition to the data received from the payroll providers, the Return Review Program (RRP) also had access to wage and withholding information from Forms W-2 transmitted by the Social Security Administration. Upon receipt and posting to the Information Returns Master File, the data was used by the RRP to identify questionable returns that may have been potentially fraudulent. The RRP programming became active on January 19, 2016. No new programming is required to take advantage of the wage and withholding information that will be due by January 31, 2017, for the 2016 tax year.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 2
Develop criteria to identify and evaluate for fraud potential tax returns *******2*****
**********************2****************.

CORRECTIVE ACTION
We agree with this recommendation. On June 13, 2016, a new business rule was implemented within the Dependent Database *******************2************
**************2***********************************.

IMPLEMENTATION DATE
Implemented

2

RESPONSIBLE OFFICIAL
Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 3
Develop a process to timely use State lead data as another characteristic in evaluating tax returns during processing to identify potential identity theft tax returns.

CORRECTIVE ACTION
We agree with this recommendation. On January 8, 2017, programming was implemented within the RRP that permits it to consider previous State lead data in informing the teams responsible for evaluating filter and model effectiveness.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 4
Use actual tax return data to identify the refund amount associated with e-filed rejected tax returns when computing revenue protected, exclude rejected e-filed tax returns that do not claim a refund, and accurately account for tax returns with multiple reject reasons.

CORRECTIVE ACTION
We agree with this recommendation. For the 2015 Identity Theft Taxonomy report, issued on November 29, 2016, the methodology was modified to count only one rejected tax return when multiple rejections are logged, and to exclude rejected returns that do not claim refunds.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 5
Review both the protected and unprotected revenue to ensure that duplicated tax returns are removed.

CORRECTIVE ACTION
For the 2015 Identity Theft Taxonomy report, issued on November 29, 2016, the methodology was modified to remove the duplications that occurred when potentially fraudulent returns were selected by more than one fraud detection system.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 6
Exclude tax returns from potential undetected identity theft when mismatches of tax return income are due to amended or duplicate income documents.

CORRECTIVE ACTION
We agree with this recommendation and have made improvements in the recently issued 2015 Identity Theft Taxonomy report of protected and unprotected identity theft refund fraud. The methodological reporting changes partially address the estimation errors associated with amended tax returns or duplicate income documents. We will further revise the methodology to improve the accuracy of the unprotected identity theft range estimate. The Taxonomy is an annual report and, although we are working to implement the corrective actions for the 2017 report, setting an implementation date of September 2018 will ensure that we provide for sufficient time for any additional analysis and methodology modifications to be completed.

IMPLEMENTATION DATE
September 15, 2018

RESPONSIBLE OFFICIAL
Director, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.